⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－81043

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開 昭和61年(1986)4月24日
H 04 L 9/00		Z－7240－5K	

審査請求 未請求 発明の数 1 （全3頁）

⑤4発明の名称　パケット通信における暗号処理方式

⑳特　願 昭59－203110

㉒出　願 昭59(1984)9月28日

㉒発明者　東　充宏　川崎市中原区上小田中1015番地　富士通株式会社内

㉒発明者　小笠原　弘二　川崎市中原区上小田中1015番地　富士通株式会社内

㉒発明者　秋山　良太　川崎市中原区上小田中1015番地　富士通株式会社内

㉑出願人　富士通株式会社　川崎市中原区上小田中1015番地

㉔代理人　弁理士　松岡　宏四郎

明　細　書

1. 発明の名称

パケット通信における暗号処理方式

2. 特許請求の範囲

収容パケット端末装置間を交換接続するパケット交換網において、送信側のパケット端末装置は送信パケット内に含まれるデータを暗号化し、復号化に必要な情報を付加して前記パケット交換網に送出し、受信側のパケット端末装置は該パケット交換網から到着する受信パケットの送信元端末装置を識別し、該受信パケットに含まれる前記復号化に必要な情報に基づき暗号化データを復号化することを特徴とするパケット通信における暗号処理方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明はパケット交換網を経由して伝達されるデータを暗号化可能とするパケット通信における暗号処理方式に関す。

近年データ通信の発展に伴い、伝送されるデータの機密保護が重要視されつつある。

〔従来の技術〕

第3図は従来ある暗号処理方式の一例を示す図である。

第3図においては、端末装置1および2が伝送路3を介して固定的に接続されている。かかる状態で、端末装置1から端末装置2に伝達するデータを暗号化する為には、端末装置1と伝送路3との間に暗号装置4を挿入し、また端末装置2と伝送路3との間に復号装置5を挿入し、更に暗号装置4で暗号化に使用しする鍵および初期値を予め復号装置5に通知して置く。かかる状態で、端末装置1が送出するデータは暗号装置4により所定の鍵および初期値により暗号化され、伝送路3に送出される。該暗号化されたデータは、伝送路3を経由して復号装置5に伝達される。復号装置5は、伝送路3から到着する暗号化されたデータを、暗号装置4と同一の鍵および初期値を用いて復号化し、端末装置2に伝達する。その結果端末装置2は、端末装置1が送信した通りのデータを受信

することが出来る。

〔発明が解決しようとする問題点〕

以上の説明から明らかな如く、従来ある暗号処理方式においては、送信側の端末装置1と受信側の端末装置2とは伝送路3により固定的に接続されていた。その結果復号装置5が復号化に必要な鍵および初期値は、暗号装置4が暗号化に使用する鍵および初期値と常に一致させることが可能であった。

然し端末装置1および2が伝送路3の代わりにパケット交換網を経由して交換接続される場合には、端末装置1からパケット交換網に伝達すべき交換制御情報をも含めて暗号化することは不可能であり、また端末装置2はパケット交換網に収容される端末装置1以外の端末装置からのパケットも受信する為、パケット交換網から伝達される総てのデータを復号装置5により復号化することも不可能となる。

〔問題点を解決するための手段〕

前記問題点は、収容パケット端末装置間を交換接続するパケット交換網において、送信側のパケット端末装置は送信パケット内に含まれるデータを暗号化し、復号化に必要な情報を付加して前記パケット交換網に送出し、受信側のパケット端末装置は該パケット交換網から到着する受信パケットの送信元端末装置を識別し、該受信パケットに含まれる前記復号化に必要な情報に基づき暗号化データを復号化することを特徴とする本発明により解決される。

〔作用〕

即ち本発明によれば、送信側のパケット端末装置はパケット交換網に送出するパケットの内、受信側のパケット端末装置に伝達すべきデータのみを暗号化し、暗号化されたデータを受信側で復号化するに必要な情報、例えば暗号化に使用した鍵或いは初期値を示す諸情報を付加し、パケット交換網が交換制御に必要な情報は暗号化すること無くパケット交換網に送出する。パケット交換網は暗号化されぬ交換制御情報に基づき暗号化されたデータおよび暗号化情報を受信側のパケット端末装置に伝達する。受信側のパケット端末装置においては、送信側のパケット端末装置を識別すると共に受信した前記復号化に必要な情報に基づき暗号化されたデータを復号化する。その結果パケット交換網を経由して伝達されるパケット内のデータは暗号化することが可能となり、機密保護が可能となる。

〔実施例〕

以下、本発明の一実施例を図面により説明する。第1図は本発明の一実施例によるパケット通信における暗号処理方式を示す図であり、第2図は第1図におけるパケット形式の一例を示す図である。

第1図においては、パケット端末装置7および8がパケット交換網6に収容されている。

今パケット端末装置7が、パケット交換網6を介してパケット端末装置8にデータを暗号化して伝達することを希望し、暗号部71にデータを伝達する。暗号部71は、鍵記憶部72内に設けられている鍵テーブル721から鍵識別符号KIDに対応する鍵を抽出し、所要の初期値IVを用いて伝達されたデータを暗号化して暗号化データEDを作成し、自端末装置7を識別する発信者識別符号UID、暗号化に使用した鍵を鍵テーブル721から抽出するに用いた鍵識別符号KIDおよび初期値IVと共に組立部73に伝達する。組立部73は、暗号部71から伝達された発信者識別符号UID、鍵識別符号KID、初期値IVおよび暗号化データEDにデータ長DLを付加してパケットのデータ部を構成し、フラグシーケンスF、アドレスフィールドA、制御フィールドCおよびフレームチェックシーケンスFCSを付加して第2図に示す如き形式のパケットを構成し、パケット交換網6に送出する。

パケット交換網6は、パケット端末装置7から伝達されたパケットのアドレスフィールドAおよび制御フィールドCを分析し、宛先のパケット端末装置8に送達する。

パケット端末装置8においては、分解部81がパケット交換網6から到着するパケットを分解し、データ部に含まれる発信者識別符号UIDおよび

鍵識別符号ＫＩＤを抽出し、鍵記憶部８２に伝達すると共に、初期値ＩＶおよび暗号化データＥＤを復号部８３に伝達する。鍵記憶部８２は、各送信側パケット端末装置７等が鍵記憶部７２等に保有すると同一の鍵テーブル８２１乃至８２ｎを具備しており、分解部８１から伝達された発信者識別符号ＵＩＤに対応する鍵テーブル（例えば８２１）を求め、該鍵テーブル８２１から鍵識別符号ＫＩＤに基づき送信側パケット端末装置７が鍵テーブル７２１から抽出したと同一の鍵を抽出し、復号部８３に伝達する。復号部８３は、鍵記憶部８２から伝達された鍵および分解部８１から伝達された初期値ＩＶを用いて、分解部８１から伝達された暗号化データＥＤを復号化し、送信側パケット端末装置７が暗号部７１に入力したと同一のデータを得る。

以上の説明から明らかな如く、本実施例によれば、パケット端末装置７からパケット端末装置８には暗号化データＥＤが発信者識別符号ＵＩＤ、鍵識別符号ＫＩＤおよび初期値ＩＶと共に伝達され、受信側パケット端末装置８は暗号化データＥＤを復号化可能となる。なおパケット交換網６がパケットをパケット端末装置８に伝達するに必要なアドレスフィールドＡ或いは制御フィールドＣに含まれる交換制御情報は暗号化されること無くパケット端末装置７から送出される為、パケット交換網６は該パケットを確実にパケット端末装置８に送達可能となる。

なお、第１図および第２図はあく迄本発明の一実施例に過ぎず、例えばパケット端末装置７および８の構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。また第１図において使用されるパケット形式は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。

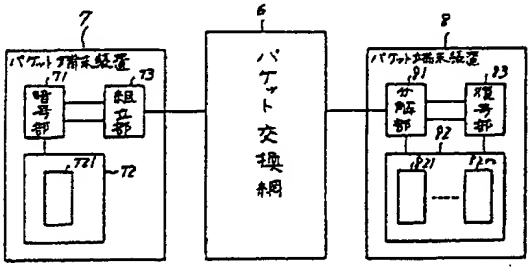
〔発明の効果〕

以上、本発明によれば、前記パケット交換網において、収容パケット端末装置間で任意に暗号化データが伝達可能となり、当該パケット交換網の機密保護性が向上する。

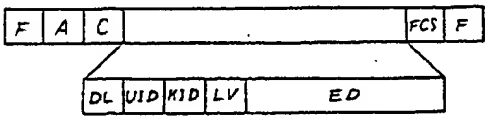
4. 図面の簡単な説明

第１図は本発明の一実施例によるパケット通信における暗号処理方式を示す図、第２図は第１図におけるパケット形式の一例を示す図、第３図は従来ある暗号処理方式の一例を示す図である。

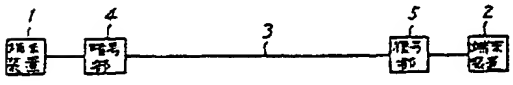
図において、１および２は端末装置、３は伝送路、４は暗号装置、５は復号装置、６はパケット交換網、７および８はパケット端末装置、７１は暗号部、７２および８２は鍵記憶部、７３は組立部、８１は分解部、８３は復号部、７２１および８２１乃至８２ｎは鍵テーブル、Ａはアドレスフィールド、Ｃは制御フィールド、ＤＬはデータ長ＥＤは暗号化データ、Ｆはフラグシーケンス、ＦＣＳはフレームチェックシーケンス、ＩＶは初期値、ＫＩＤは鍵識別符号、ＵＩＤは発信者識別符号、を示す。



第 1 図



第 2 図



第 3 図

代理人　弁理士　松岡宏四郎